JOURNAL OF COMBINATORIAL THEORY, Series A 77, 339–343 (1997)
ARTICLE NO. TA972715

NOTE

Large Product-Free Subsets of Finite Groups

Kiran S. Kedlaya*

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138

Communicated by Laci Babai

Received August 12, 1994

A subset of a group is said to be *product-free* if the product of two of its

of Babai and Sós.

Let G be a finite group of order n. A subset S of G is said to be *product-free* if, for any $x, y \in S$ (not necessarily distinct), $xy \notin S$. Define $\alpha(G)$ to be the size of the largest product-free subset of G. In [1], Babai and Sós gave a simple construction that, together with the classification of finite simple groups (CFSG), shows that $\alpha(G) > cn^{4/7}$ for some constant $c > 0$. The purpose of the present paper is to improve this lower bound as follows.

THEOREM. *There exists a constant $c > 0$ such that $\alpha(G) > cn^{11/14}$.*

We begin the proof of the theorem by recalling Lemma 7.5 of [1].

LEMMA 1. *If N is a normal subgroup of G, then $\alpha(G) \geqslant \alpha(N)[G : N]$.*

Proof. Let $\phi: G \to G/N$ be the canonical homomorphism. If S is product-free in G/N, then $\phi^{-1}(S)$ is product-free in G. ∎

Thus to prove any bound of the form $\alpha(G) > cn^t$ for $t \leqslant 1$, it suffices to consider the finite simple groups. In the case $G = \mathbb{Z}/n\mathbb{Z}$, the set $\{k, ..., 2k-1\}$, where $k = \lfloor (n+1)/3 \rfloor$, shows that $\alpha(G) > cn$. By Lemma 1, the linear lower bound also holds for all groups with cyclic factor groups, so in particular for all solvable groups.

* Correspondence should be addressed to: Kiran S. Kedlaya, 14515 Jaystone Drive, Silver Spring, MD 20905, U.S.A.

0097-3165/97 $25.00

LEMMA 2. *Let $P(G)$ denote the index of the largest proper subgroup of G. Then there exists $c>0$ such that $P(G)<c\,|G|^{3/7}$ for all nonabelian simple groups G.*

By CFSG, it suffices to verify this claim for the simple groups of Lie type (the alternating groups satisfy this by a wide margin, and the sporadic groups, being finite in number, can be accommodated by adjusting the constant). The simple groups of Lie type fall into two categories, the classical families and the exceptional families. We summarize the results for the classical and exceptional families in Tables I and II, culled from [3] (pp. 170, 175) and [4], respectively. (Note that the exponent cannot be lowered, on account of the Ree groups ${}^2G_2(q)$.) The results are given in Knuth's Θ notation: for two sequences (a_n) and (b_n), we write $a_n=\Theta(b_n)$ if there exist positive constants c_1 and c_2 such that $c_1<a_n/b_n<c_2$ for sufficiently large n.

Babai and Sós observe that $\alpha(G)\geqslant |G|/P(G)$, since any nontrivial coset of a proper subgroup of G is product-free. In light of Lemma 2, this implies $\alpha(G)\geqslant c\,|G|^{4/7}$. (Note that neither Lemma 2 nor this last inequality appear in [1], only the construction.) We shall prove a stronger result.

LEMMA 3. *For all G, $\alpha(G)\geqslant (31P(G))^{-1/2}\,|G|$.*

Proof. We prove the equivalent statement that if G acts transitively on $\Omega=\{1, ..., l\}$, where $l>31$, then $\alpha(G)\geqslant (31l)^{-1/2}\,|G|$. (For $l\leqslant 31$ the result follows from the previous estimate.)

TABLE I

Largest Subgroups of the Classical Simple Groups

Group	Lie notation	$\lvert L\rvert$	$P(L)$	$\lim_{q\to\infty} \log_{\lvert L\rvert} P(L)$	$\max_m$
$L_m(q)$ $(m\geqslant 2)$	$A_{m-1}(q)$	$\Theta(q^{m^2-1})$	$\Theta(q^{m-1})$	$\frac{1}{m+1}$	$\frac{1}{3}\approx 0.333$
$U_m(q)$ $(m\geqslant 2)$	${}^2A_{m-1}(q)$	$\Theta(q^{m^2-1})$	$\Theta(q^{2m-3})$	$\frac{2m-3}{m^2-1}$	$\frac{3}{8}\approx 0.313$
$PSp_{2m}(q)$ $(m\geqslant 2)$	$C_m(q)$	$\Theta(q^{2m^2+m})$	$\Theta(q^{2m-1})$	$\frac{2m-1}{2m^2+m}$	$\frac{3}{10}\approx 0.300$
$\Omega_{2m+1}(q)$ $(m\geqslant 3)$	$B_m(q)$	$\Theta(q^{2m^2+m)}$	$\Theta(q^{2m-1)}$	$\frac{2m-1}{2m^2+m}$	$\frac{5}{21}\approx 0.238$
$P\Omega^+_{2m}(q)$ $(m\geqslant 3)$	$D_m(q)$	$\Theta(q^{2m^2-m})$	$\Theta(q^{2m-2})$	$\frac{2m-2}{2m^2-m}$	$\frac{4}{15}\approx 0.267$
$P\Omega^-_{2m}(q)$ $(m\geqslant 2)$	${}^2D_m(q)$	$\Theta(q^{2m^2-m})$	$\Theta(q^{2m-2})$	$\frac{2m-2}{2m^2-m}$	$\frac{1}{3}\approx 0.333$

TABLE II

Largest Subgroups of the Exceptional Simple Groups

Group	$\lvert L\rvert$	$P(L)$	$\lim_{q\to\infty} \log_{\lvert L\rvert} P(L)$
$G_2(q)$	$\Theta(q^{14})$	$\Theta(q^5)$	$\frac{5}{14} \approx 0.357$
$F_4(q)$	$\Theta(q^{52})$	$\Theta(q^{15})$	$\frac{15}{52} \approx 0.288$
$E_6(q)$	$\Theta(q^{78})$	$\Theta(q^{16})$	$\frac{16}{78} \approx 0.205$
$E_7(q)$	$\Theta(q^{133})$	$\Theta(q^{27})$	$\frac{27}{133} \approx 0.203$
$E_8(q)$	$\Theta(q^{248})$	$\Theta(q^{57})$	$\frac{57}{248} \approx 0.230$
${}^2B_2(q)(q=2^{2m+1})$	$\Theta(q^5)$	$\Theta(q^2)$	$\frac{2}{5} \approx 0.400$
${}^2G_2(q)(q=3^{2m+1})$	$\Theta(q^7)$	$\Theta(q^3)$	$\frac{3}{7} \approx 0.429$
${}^2F_4(q)(q=2^{2m+1})$	$\Theta(q^{26})$	$\Theta(q^{10})$	$\frac{10}{26} \approx 0.385$
${}^3D_4(q)$	$\Theta(q^{28})$	$\Theta(q^9)$	$\frac{9}{28} \approx 0.321$
${}^2E_6(q)$	$\Theta(q^{78})$	$\Theta(q^{21})$	$\frac{21}{78} \approx 0.269$

Let T be a k-element subset of $\Omega - \{1\}$, where k shall be specified later. Let S be the set of all $g \in G$ such that $1^g \in T$ and for all $y \in T$, $y^g \notin T$. In symbols,

$$S = \bigcup_{x \in T} \{g \in G \mid 1^g = x\} - \bigcup_{y \in T} \{g \in G \mid 1^g, y^g \in T\}.$$

If $g, h \in S$, then $1^{gh} = (1^g)^h$ and since $1^g \in T$, $(1^g)^h \notin T$. Therefore S is product-free. (This generalizes the construction of Babai and Sós, which is the case $k = 1$.)

Since G acts transitively on Ω, each set in the first union has $|G|/l$ elements. Thus the first union contains $k\,|G|/l$ elements. For fixed k, if β denotes the average size of the second union over all k-element subsets T of $\{2, ..., l\}$, then the average size of S is $k\,|G|/l - \beta$, and of course, S must be at least this large for some particular T.

In passing, we note that the above application of the probabilistic method (see [2] for many more examples of the method) can be avoided if G acts 2-transitively on Ω (as is the case for a number of the simple groups). In this case the size of each set in the second union can be given explicitly, from which one can deduce that for every choice of T, S is large enough to prove the theorem. In particular, for such groups a product-free set of the claimed size can be constructed explicitly (assuming H is known).

In any case, we now establish an upper bound for β. First observe that

$$\binom{l-1}{k}\beta \leqslant \sum_{T}\sum_{y\in T} \#(g\in G \mid 1^g, y^g \in T)$$

$$= \sum_{y\neq 1}\sum_{g\in G} \#(T\subseteq \Omega - \{1\} \mid 1^g, y, y^g \in T).$$

If $1^g, y, y^g$ are distinct, this last set has $\binom{l-4}{k-3}$ elements, but if $1^g = y$ or $y^g = y$, it has $\binom{l-3}{k-2}$ elements. (To be precise, no such T exist at all unless $1^g \neq 1$ and $y^g \neq 1$, but overcounting won't hurt in deriving an upper bound.) Thus

$$\binom{l-1}{k}\beta \leqslant \binom{l-4}{k-3}\sum_{y\neq 1}|G|$$

$$+\binom{l-3}{k-2}\sum_{y\neq 1}[\#(g\in G \mid 1^g = y) + \#(g\in G \mid y^g = y)]$$

$$= \binom{l-4}{k-3}(l-1)|G| + 2\binom{l-3}{k-2}\frac{(l-1)|G|}{l},$$

again because G acts transitively. This gives

$$\frac{\beta}{|G|} \leqslant \frac{k(k-1)}{l(l-2)(l-3)}[l(k-2)+2(l-3)]$$

$$\leqslant \frac{k(k-1)}{l(l-2)(l-3)}lk \leqslant \frac{k^3}{(l-2)^2}.$$

We conclude that for $k\in\{1, ..., l-1\}$, there exists a product-free subset S of G such that

$$|S| \geqslant \left(\frac{k}{l} - \frac{k^3}{(l-2)^2}\right)|G|.$$

Finally, we choose k to maximize this expression. Put $k = \lfloor (l-2)(3l)^{-1/2}\rfloor$; then

$$|S| \geqslant \left(\frac{l-2}{3^{1/2}l^{3/2}} - \frac{1}{l} - \frac{l-2}{(3l)^{3/2}}\right)|G|$$

$$= \frac{2l-\sqrt{27l}-4}{(3l)^{3/2}}|G| > (31l)^{-1/2}|G|,$$

where the last inequality assumes $l > 31$. ∎

Lemmas 2 and 3 together imply that $\alpha(G) > cn^{11/14}$ for simple groups, which by Lemma 1 suffices to prove the theorem in full.

ACKNOWLEDGMENT

This paper was written during the 1994 Research Experience for Undergraduates at the University of Minnesota, Duluth, directed by Joseph Gallian and sponsored by the National Science Foundation (Grant DMS-9225045) and the National Security Agency (Grant MDA 904-91-H-0036).

The author thanks Larry Finkelstein for observing that the groups $L_2(q)$ are not the worst case in Lemma 2, correcting an error in an earlier version of this paper (also implicit in Remark 7.11 of [1]). We also thank Aner Shalev for providing the manuscript of [4], which enabled us to determine the correct exponent in Lemma 2.

REFERENCES

1. L. Babai and V. T. Sós, Sidon sets in groups and induced subgraphs of Cayley graphs, *Europ. J. Combin.* **6** (1985), 101–114.
2. P. Erdős and J. Spencer, "Probabilistic Methods in Combinatorics," Akadémiai Kiadó, Budapest, 1974.
3. P. Kleidman and M. Liebeck, "The Subgroup Structure of the Finite Classical Groups," Cambridge Univ. Press, Cambridge, 1990.
4. M. W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, *J. Algebra*, to appear.